

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

| High Vulnerabilities | | | | |
|--|---|-----------------------|---------------------|--|
| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
| Adaptive Technology Resource Centre -- ATutor | SQL injection vulnerability in index.php in ATutor 1.5.3 allows remote attackers to execute arbitrary SQL commands via the fid parameter. | unknown 2006-07-18 | 7.0 | CVE-2006-3662 BUGTRAQ BID XF |
| Cisco -- Unified CallManager | Buffer overflow in Cisco Unified CallManager (CUCM) 5.0(1) through 5.0(3a) allows remote attackers to execute arbitrary code via a long hostname in a SIP request, aka bug CSCsd96542. | unknown 2006-07-18 | 7.0 | CVE-2006-3594 CISCO FRSIRT SECUNIA XF |
| Cisco -- Router Web Setup | The default configuration of IOS HTTP server in Cisco Router Web Setup (CRWS) before 3.3.0 build 31 does not require credentials, which allows remote attackers to access the server with arbitrary privilege levels, aka bug CSCsa78190. | unknown 2006-07-18 | 7.0 | CVE-2006-3595 CISCO BID FRSIRT SECUNIA XF |
| Codeworks -- Gnomedia SubberZ | PHP remote file inclusion vulnerability in user-func.php in Codeworks Gnomedia SubberZ[Lite] allows remote attackers to execute arbitrary PHP code via a URL in the myadmindir parameter. | unknown 2006-07-21 | 7.0 | CVE-2006-3689 BUGTRAQ BID |
| D-Link -- DI-604 Broadband Router D-Link -- | Stack-based buffer overflow in the Universal Plug and Play (UPnP) service in D-Link DI-524, DI-604 Broadband Router, DI-624, D-Link | unknown 2006-07-21 | 7.0 | CVE-2006-3687 OTHER-REF FRSIRT |

| | | | | |
|--|---|-----------------------|----------------------|--|
| WBR-2310 RangeBooster G Router D-Link -- DI-624 D-Link -- WBR-1310 Wireless G Router D-Link -- DI-524 D-Link -- EBR-2310 Ethernet Broadband Router D-Link -- DI-784 | DI-784, WBR-1310 Wireless G Router, WBR-2310 RangeBooster G Router, and EBR-2310 Ethernet Broadband Router allows remote attackers to execute arbitrary code via a long M-SEARCH request to UDP port 1900. | | | SECUNIA |
| DotNetNuke -- DotNetNuke | ** UNVERIFIABLE ** Unspecified vulnerability in an unspecified DNN Modules module for DotNetNuke (.net nuke) allows remote attackers to gain privileges via unspecified vectors, as used in an attack against the Microsoft France web site. NOTE: due to the lack of details and uncertainty about which product is affected, this claim is not independently verifiable. | unknown 2006-07-18 | 10.0 | CVE-2006-3601 OTHER-REF SECTRAK |
| Dynamic Universal Music Bibliotheque -- DUMB | Heap-based buffer overflow in the it_read_envelope function in Dynamic Universal Music Bibliotheque (DUMB) 0.9.3 and earlier, and current CVS as of 20060716, allows user-complicit attackers to execute arbitrary code via a ".it" (Impulse Tracker) file with an enveloper with a large number of nodes. | unknown 2006-07-18 | 8.0 | CVE-2006-3668 ALTERVISTA FRSIRT SECUNIA |
| Eskolar CMS -- Eskolar CMS | Multiple SQL injection vulnerabilities in Eskolar CMS 0.9.0.0 allow remote attackers to execute arbitrary SQL commands via the (1) gr_1_id, (2) gr_2_id, (3) gr_3_id, and (4) doc_id parameters in (a) index.php; the (5) uid and (6) pwd parameters in (b) php/esa.php; and possibly other vectors related to files in php/lib/ including (c) del.php, (d) download_backup.php, (e) navig.php, (f) restore.php, (g) set_12.php, (h) set_14.php, and (i) upd_doc.php. | unknown 2006-07-21 | 7.0 | CVE-2006-3727 OTHER-REF BID FRSIRT SECUNIA |
| Ethereal Group -- Ethereal | Multiple format string vulnerabilities in Wireshark (formerly Ethereal) 0.10.x to 0.99.0 allow remote attackers to cause a denial of service and possibly execute arbitrary code via the (1) ANSI MAP, (2) Checkpoint FW-1, (3) MQ, (4) XML, and (5) NTP dissectors. | unknown 2006-07-21 | 7.0 | CVE-2006-3628 WIRESHARK |
| Ethereal Group -- Ethereal | Multiple off-by-one errors in Wireshark (formerly Ethereal) 0.9.7 to 0.99.0 have unknown impact and remote attack vectors via the (1) NCP NMAS and (2) NDPS dissectors. | unknown 2006-07-21 | 7.0 | CVE-2006-3630 WIRESHARK |

| | | | | |
|--|---|--------------------------|----------------------|--|
| Ethereal Group -- Ethereal | Buffer overflow in Wireshark (formerly Ethereal) 0.8.16 to 0.99.0 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the NFS dissector. | unknown 2006-07-21 | 7.0 | CVE-2006-3632 WIRESHARK |
| FatWire -- Content Server | FatWire Content Server 5.5.0 allows remote attackers to bypass access restrictions and obtain administrative privileges via unspecified attack vectors in the authentication process. | 2006-05-31 2006-07-21 | 10.0 | CVE-2006-3679 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA |
| Flipper Poll -- Flipper Poll | PHP remote file inclusion vulnerability in poll.php in Flipper Poll 1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter. | unknown 2006-07-21 | 7.0 | CVE-2006-3683 BUGTRAQ BUGTRAQ BID FRSIRT SECTrack SECUNIA XF |
| Francisco Charrua -- Photo-Gallery | SQL injection vulnerability in Room.php in Francisco Charrua Photo-Gallery 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown 2006-07-21 | 7.0 | CVE-2006-3688 BID FRSIRT SECUNIA |
| FreeType -- FreeType | Integer overflow in FreeType before 2.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors, as demonstrated by the Red Hat bad1.pcf test file, due to a partial fix of CVE-2006-1861. | unknown 2006-07-21 | 7.0 | CVE-2006-3467 OTHER-REF REDHAT |
| Hyper Estraier -- Hyper Estraier | Cross-site request forgery (CSRF) vulnerability in the communicate function in estmaster.c for Hyper Estraier before 1.3.3 allows remote attackers to perform unauthorized actions as other users via unknown vectors. | unknown 2006-07-18 | 7.0 | CVE-2006-3671 SOURCEFORGE FRSIRT SECUNIA |
| Koobi -- Koobi Pro | SQL injection vulnerability in the showtopic module in Koobi Pro CMS 5.6 allows remote attackers to execute arbitrary SQL commands via the toid parameter. | unknown 2006-07-18 | 7.0 | CVE-2006-3621 BID SECTrack |
| Lavasoft -- Lavasoft Personal Firewall Novell -- Novell Client Firewall Agnitum -- Outpost Firewall | Outpost Firewall Pro 3.51.759.6511 (462), as used in (1) Lavasoft Personal Firewall 1.0.543.5722 (433) and (2) Novell Border Manager Novell Client Firewall 2.0, allows local users to gain privileges and execute commands via the "open folder" option when no instance of explorer.exe is running, possibly related to the ShellExecute API function. NOTE: this might be a vulnerability in Microsoft Windows and | 2006-07-10 2006-07-21 | 7.0 | CVE-2006-3697 OTHER-REF BID BID FRSIRT FRSIRT SECUNIA SECUNIA |

| | | | | |
|--|---|-----------------------|---------------------|---|
| | explorer.exe instead of the firewall. | | | |
| LibVNCServer -- LibVNCServer | auth.c in LibVNCServer 0.7.1 allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server, a different issue than CVE-2006-2369. | unknown 2006-07-18 | 7.0 | CVE-2006-2450 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA |
| Microsoft -- ISA Server | Microsoft Internet Security and Acceleration (ISA) Server 2004 allows remote attackers to bypass file extension filters via a request with a trailing "#" character. NOTE: as of 20060715, this could not be reproduced by third parties. | unknown 2006-07-18 | 7.0 | CVE-2006-3652 BUGTRAQ BUGTRAQ BID |
| MiniBB -- MiniBB Forum 1.5a | Multiple PHP remote file inclusion vulnerabilities in MiniBB Forum 1.5a and earlier allow remote attackers to execute arbitrary PHP code via a URL in the absolute_path parameter to (1) components/com_minibb.php or (2) components/minibb/index.php. | unknown 2006-07-21 | 7.0 | CVE-2006-3690 BUGTRAQ BID XF |
| myiosoft.com -- AjaxPortal | SQL injection vulnerability in AjaxPortal 3.0, with magic_quotes_gpc disabled, allows remote attackers to execute arbitrary SQL commands via the 'Search' field, a different vulnerability than CVE-2006-3515. | unknown 2006-07-18 | 7.0 | CVE-2006-3666 BUGTRAQ OSVDB SECUNIA XF |
| Oracle -- Oracle Database Server | Multiple unspecified vulnerabilities in Oracle Database 10.1.0.5 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB01 for Change Data Capture (CDC) component and (2) DB03 for Data Pump Metadata API. | unknown 2006-07-21 | 7.0 | CVE-2006-3698 OTHER-REF OTHER-REF BID FRSIRT |
| Orbitcoders -- OrbitMATRIX | index.php in Orbitcoders OrbitMATRIX 1.0 allows remote attackers to trigger a SQL error via the page_name parameter, possibly due to a SQL injection vulnerability. | unknown 2006-07-18 | 7.0 | CVE-2006-3614 BUGTRAQ XF |
| PHP-Nuke -- PHP-Nuke Sections Module | SQL injection vulnerability in the Sections module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the artid parameter in a viewarticle op. | unknown 2006-07-18 | 7.0 | CVE-2006-3598 BUGTRAQ |
| PHP-Nuke -- PHP-Nuke Advanced Classified Module | SQL injection vulnerability in the Nuke Advanced Classifieds module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the id_ads parameter in an EditAds op. | unknown 2006-07-18 | 7.0 | CVE-2006-3599 BUGTRAQ |
| Pixelated By Lev -- Pixelated By Lev Guestbook | SQL injection vulnerability in pblguestbook.php in Pixelated By Lev (PBL) Guestbook 1.32 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) name, (2) email, (3) website, (4) comments, (5) rate, and (6) private parameters. | unknown 2006-07-18 | 7.0 | CVE-2006-3618 BUGTRAQ OTHER-REF XF |

| | | | | |
|---|--|--------------------------|---------------------|--|
| Rabox -- Winlpd | Stack-based buffer overflow in Winlpd 1.26 allows remote attackers to execute arbitrary code via a long string in a request to TCP port 515. | 2006-07-15 2006-07-18 | 7.0 | CVE-2006-3670 OTHER-REF Milw0rm FRSIRT SECUNIA |
| Seyeon -- FlexWATCH Network Camera | Directory traversal vulnerability in FlexWATCH Network Camera 3.0 and earlier allows remote attackers to bypass access restrictions for (1) admin/aindex.asp or (2) admin/aindex.html via a .. (dot dot) and encoded / (%2f) sequence in the URL. | unknown 2006-07-18 | 7.0 | CVE-2006-3604 BUGTRAQ OTHER-REF BID SECUNIA XF |
| Silentweb -- ListMessenger | PHP remote file inclusion vulnerability in enduser/listmessenger.php in ListMessenger 0.9.3 allows remote attackers to execute arbitrary PHP code via a URL in the lm_path parameter. | unknown 2006-07-21 | 7.0 | CVE-2006-3692 BUGTRAQ BID |
| SoftComplex -- PHP Event Calendar | PHP remote file inclusion vulnerability in calendar.php in SoftComplex PHP Event Calendar 1.4 allows remote attackers to execute arbitrary PHP code via a URL in the path_to_calendar parameter, which overwrites the \$path_to_calendar variable from an extract function call. | 2006-07-13 2006-07-21 | 7.0 | CVE-2006-3684 OTHER-REF BID |
| Sybase -- Financial Fusion Consumer Banking Suite | Unspecified vulnerability in Sybase/Financial Fusion Consumer Banking Suite versions before 20060706 has unknown impact and remote attack vectors. | unknown 2006-07-18 | 7.0 | CVE-2006-3667 OTHER-REF SECUNIA |
| Ubuntu -- Ubuntu Linux | passwd before 1:4.0.13 on Ubuntu 6.06 LTS leaves the root password blank instead of locking it when the administrator selects the "Go Back" option after the final "Installation complete" message and uses the main menu, which causes the password to be zeroed out in the installer's memory. | unknown 2006-07-18 | 7.0 | CVE-2006-3597 UBUNTU SECUNIA |
| VBZoom -- VBZoom | Multiple SQL injection vulnerabilities in VBZoom 1.11 and earlier allow remote attackers to execute arbitrary SQL commands via the UserID parameter to (1) ignore-pm.php, (2) sendmail.php, (3) reply.php or (4) sub-join.php. | unknown 2006-07-21 | 7.0 | CVE-2006-3691 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BID |

[Back to top](#)

| Medium Vulnerabilities | | | | |
|---------------------------|---|-----------------------|---------------------|--|
| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
| Chamberland Technology -- | Multiple cross-site scripting (XSS) vulnerabilities in Chamberland Technology ezWaiter 3.0 Online | unknown 2006-07-18 | 4.7 | CVE-2006-3613 BUGTRAQ |

| | | | | |
|--------------------------------------|--|--------------------------|---------------------|---|
| ezWaiter Online | and possibly Enterprise Software (aka enterprise edition) allow remote attackers to inject arbitrary web script or HTML via the (1) itemfor (aka "Who is this item for?") and (2) special (aka "Special Instructions") parameters to item.php, which is accessed from showorder.php, or (3) unspecified parameters to the login form at login.php. | | | BID |
| Cisco -- Unified CallManager | Unspecified vulnerability in the command line interface (CLI) in Cisco Unified CallManager (CUCM) 5.0(1) through 5.0(3a) allows local users to execute arbitrary commands with elevated privileges via unspecified vectors, involving "certain CLI commands," aka bug CSCse11005. | unknown 2006-07-18 | 4.9 | CVE-2006-3592 CISCO FRSIRT SECUNIA XF |
| Czaries Network -- CzarNews | PHP remote file inclusion vulnerability in CzarNews 1.12 through 1.14 allows remote attackers to execute arbitrary PHP code via a URL in the tpath parameter to cn_config.php. NOTE: the news.php vector is already covered by CVE-2005-0859. | unknown 2006-07-21 | 5.6 | CVE-2006-3685 OTHER-REF SECUNIA |
| Edgework Software -- Trac | Unspecified vulnerability in Trac before 0.9.6 allows remote attackers to cause a denial of service or obtain sensitive information via unspecified vectors involving "reStructuredText". NOTE: this might be related to CVE-2006-3458. | unknown 2006-07-21 | 4.7 | CVE-2006-3695 OTHER-REF FRSIRT SECTRACK |
| Finjan -- Finjan Appliance 5100/8100 | Finjan Appliance 5100/8100 NG 8.3.5 stores passwords in plaintext in a backup file, which allows local users to gain privileges. | unknown 2006-07-18 | 4.9 | CVE-2006-3663 FULLDISC BID XF |
| InterVations -- FileCOPA FTP Server | Buffer overflow in FileCOPA FTP Server before 1.01 released on 18th July 2006, allows remote authenticated attackers to execute arbitrary code via a long argument to the LIST command. | 2006-07-17 2006-07-21 | 4.2 | CVE-2006-3726 OTHER-REF FRSIRT SECUNIA |
| libtunepimp -- libtunepimp | Multiple stack-based buffer overflows in the LookupTRM::lookup function in libtunepimp 0.4.2 allow remote user-complicit attackers to cause a denial of service (application crash) and possibly execute code via a long (1) Album release date (MBE_ReleaseGetDate), (2) data, or (3) error strings. | unknown 2006-07-18 | 5.6 | CVE-2006-3600 OTHER-REF UBUNTU BID SECUNIA SECUNIA |
| Linux -- Linux kernel | Race condition in Linux kernel 2.6.17.4 and earlier allows local users to gain root privileges by using prctl with PR_SET_DUMPABLE in a way that causes /proc/self/environ to become setuid root. | unknown 2006-07-18 | 5.6 | CVE-2006-3626 FULLDISC |
| Microsoft -- PowerPoint | Unspecified vulnerability in mso.dll, as used by Microsoft PowerPoint 2000 through 2003, allows remote user-complicit attackers to execute | unknown 2006-07-14 | 5.6 | CVE-2006-3590 OTHER-REF OTHER-REF |

| | | | | |
|----------------------------------|---|-----------------------|---------------------|--|
| | arbitrary commands via a crafted PPT file, which causes a "memory corruption error," and exploited by Trojan.PPDropper.B. NOTE: As of 20060714, due to the vagueness of the initial disclosure, it is uncertain whether this is related to CVE-2006-1540 or CVE-2006-3493. | | | OTHER-REF CERT-VN BID FRSIRT |
| Microsoft -- PowerPoint | Unspecified vulnerability in mso.dll in Microsoft PowerPoint 2003 allows user-complicit attackers to execute arbitrary code via a crafted PowerPoint file. NOTE: due to the lack of available details as of 20060717, it is unclear how this is related to CVE-2006-3656, CVE-2006-3660, and CVE-2006-3590, although it is possible that they are all different. | unknown 2006-07-18 | 5.6 | CVE-2006-3655 BUGTRAQ BID FRSIRT |
| Microsoft -- PowerPoint | Unspecified vulnerability in Microsoft PowerPoint 2003 has unknown impact and user-complicit attack vectors related to powerpnt.exe. NOTE: due to the lack of available details as of 20060717, it is unclear how this is related to CVE-2006-3655, CVE-2006-3656, and CVE-2006-3590, although it is possible that they are all different. | unknown 2006-07-18 | 5.6 | CVE-2006-3660 BUGTRAQ BID FRSIRT |
| Oracle -- Oracle Database Server | Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.0.1.5 and 9.2.0.6 has unknown impact and attack vectors, aka Oracle Vuln# DB02. | unknown 2006-07-21 | 4.9 | CVE-2006-3699 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Multiple unspecified vulnerabilities in Oracle Database 9.2.0.6 and 10.1.0.4 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB04 for Web Distributed Authoring and Versioning (DAV) and (2) DB23 for XMLDB. | unknown 2006-07-21 | 4.9 | CVE-2006-3700 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Unspecified vulnerability in the Dictionary component in Oracle Database 8.1.7.4, 9.0.1.5, and 9.2.0.6 has unknown impact and attack vectors, aka Oracle Vuln# DB05. | unknown 2006-07-21 | 4.9 | CVE-2006-3701 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Multiple unspecified vulnerabilities in Oracle Database 8.1.7.4, 9.0.1.5, 9.2.0.7, 10.1.0.5, and 10.2.0.2 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB06 in Export; (2) DB08, (3) DB09, (4) DB10, (5) DB11, (6) DB12, (7) DB13, (8) DB14, and (9) DBC01 for OCI; (10) DB16 for Query Rewrite/Summary Mgmt; (11) DB17, (12) DB18, (13) DB19, (14) DBC02, (15) DBC03, and (16) DBC04 for RPC; and (17) DB20 for Semantic Analysis. | unknown 2006-07-21 | 4.9 | CVE-2006-3702 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Unspecified vulnerability in InterMedia for Oracle Database 9.0.1.5, 9.2.0.6, and 10.1.0.4 has | unknown 2006-07-21 | 4.9 | CVE-2006-3703 OTHER-REF |

| | | | | |
|---|--|-----------------------|---------------------|--|
| | unknown impact and attack vectors, aka oracle Vuln# DB07. | | | OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Unspecified vulnerability in the Oracle ODBC Driver for Oracle Database 10.1.0.4 has unknown impact and attack vectors, aka Oracle Vuln# 10.1.0.4. | unknown 2006-07-21 | 4.9 | CVE-2006-3704 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Database Server | Multiple unspecified vulnerabilities in Oracle Database 10.1.0.5 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB21 for Statistics and (2) DB22 for Upgrade & Downgrade. | unknown 2006-07-21 | 4.9 | CVE-2006-3705 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Application Server 10g | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3 has unknown impact and attack vectors, aka Oracle Vuln# AS01. | unknown 2006-07-21 | 4.9 | CVE-2006-3706 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Application Server 10g | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3 and 9.0.3.1 has unknown impact and attack vectors, aka Oracle Vuln# AS02. | unknown 2006-07-21 | 4.9 | CVE-2006-3707 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Application Server 10g | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3, 9.0.3.1, 9.0.4.2, 10.1.2.0.2, and 10.1.2.1 has unknown impact and attack vectors, aka Oracle Vuln# AS03. | unknown 2006-07-21 | 4.9 | CVE-2006-3708 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle9i Application Server Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3, 9.0.3.1, and 10.1.2.0.0 has unknown impact and attack vectors, aka Oracle Vuln# AS04. | unknown 2006-07-21 | 4.9 | CVE-2006-3709 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle9i Application Server Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3, 9.0.3.1, 9.0.4.2, and 10.1.2.0.0 has unknown impact and attack vectors, aka Oracle Vuln# (1) AS05 and (2) AS08. | unknown 2006-07-21 | 4.9 | CVE-2006-3710 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle9i Application Server Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.2.3, 9.0.3.1, and 9.0.4.1 has unknown impact and attack vectors, aka Oracle Vuln# AS06. | unknown 2006-07-21 | 4.9 | CVE-2006-3711 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 9.0.4.2 and 10.1.2.0.0 has unknown impact and attack vectors, aka Oracle Vuln# AS07. | unknown 2006-07-21 | 4.9 | CVE-2006-3712 OTHER-REF OTHER-REF BID FRSIRT |

| | | | | |
|--|---|-----------------------|---------------------|--|
| Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 10.1.3.0 has unknown impact and attack vectors, aka Oracle Vuln# AS09. | unknown 2006-07-21 | 4.9 | CVE-2006-3713 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle10g Application Server | Unspecified vulnerability in OC4J for Oracle Application Server 10.1.2.0.2 and 10.1.2.1 has unknown impact and attack vectors, aka Oracle Vuln# AS10. | unknown 2006-07-21 | 4.9 | CVE-2006-3714 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Collaboration Suite Release 1 | Unspecified vulnerability in Calendar for Oracle Collaboration Suite 10.1.2 has unknown impact and attack vectors, aka Oracle Vuln# OCS01. | unknown 2006-07-21 | 4.9 | CVE-2006-3715 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle E-Business Suite and Applications | Multiple unspecified vulnerabilities in Oracle E-Business Suite and Applications 11.5.10CU2 have unknown impact and attack vectors, aka Oracle Vuln# (1) APPS01 for Internet Expenses; (2) APPS02, (3) APPS05, (4) APPS06, (5) APPS07, (6) APPS08, (7) APPS09, and (8) APPS10 for Oracle Application Object Library; (9) APPS11, (10) APPS12, and (11) APPS13 for Oracle Applications Technology Stack; (12) APPS14 for Oracle Call Center Technology; (13) APPS15 for Oracle Common Applications; (14) APPS18 for Oracle Self-Service Web Applications; and (15) APPS19 for Oracle Workflow Cartridge. | unknown 2006-07-21 | 4.9 | CVE-2006-3716 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle E-Business Suite and Applications | Multiple unspecified vulnerabilities in Oracle E-Business Suite and Applications 11.5.9 have unknown impact and attack vectors, aka Oracle Vuln# (1) APPS03 and (2) APPS04 for Oracle Application Object Library; and (3) APPS20 for Oracle XML Gateway. | unknown 2006-07-21 | 4.9 | CVE-2006-3717 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Exchange | Multiple unspecified vulnerabilities in Oracle Exchange for Oracle E-Business Suite and Applications 6.2.4 have unknown impact and attack vectors, aka Oracle Vuln# (1) APPS16 and (2) APPS17. | unknown 2006-07-21 | 4.9 | CVE-2006-3718 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Enterprise Manager | Unspecified vulnerability in CORE: Repository for Oracle Enterprise Manager 9.0.1.0 and 9.2.0.1 has unknown impact and attack vectors, aka Oracle Vuln# EM01. | unknown 2006-07-21 | 4.9 | CVE-2006-3719 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- Oracle Enterprise Manager | Unspecified vulnerability in Enterprise Config Management for Oracle Enterprise Manager 10.1.0.3 has unknown impact and attack vectors, aka Oracle Vuln# EM02. | unknown 2006-07-21 | 4.9 | CVE-2006-3720 OTHER-REF OTHER-REF BID |

| | | | | |
|--|---|-----------------------|---------------------|---|
| | | | | FRSIRT |
| Oracle -- Oracle Enterprise Manager | Multiple unspecified vulnerabilities in Oracle Management Service for Oracle Enterprise Manager 10.1.0.5 and 10.2.0.1 have unknown impact and attack vectors, aka Oracle Vuln# EM03 and EM04. | unknown 2006-07-21 | 4.9 | CVE-2006-3721 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- PeopleSoft Enterprise | Unspecified vulnerability in PeopleSoft Enterprise Portal for Oracle PeopleSoft Enterprise Portal 8.4 Bundle #16, 8.8 Bundle #10, and 8.9 Bundle #3 has unknown impact and attack vectors, aka Oracle Vuln# PSE01. | unknown 2006-07-21 | 4.9 | CVE-2006-3722 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- PeopleSoft Enterprise | Unspecified vulnerability in PeopleSoft Enterprise Portal for Oracle PeopleSoft Enterprise Portal 8.8 with Enforcer Portal Pack Bundle #10 and 8.9 Bundle #3 has unknown impact and attack vectors, aka Oracle Vuln# PSE02. | unknown 2006-07-21 | 4.9 | CVE-2006-3723 OTHER-REF OTHER-REF BID FRSIRT |
| Oracle -- JD Edwards EnterpriseOne | Unspecified vulnerability in JD Edwards HTML Server for Oracle OneWorld Tools EnterpriseOne Tools 8.95 and 8.96 has unknown impact and attack vectors, aka Oracle Vuln# JDE01. | unknown 2006-07-21 | 4.9 | CVE-2006-3724 OTHER-REF OTHER-REF BID FRSIRT |
| Phorum -- Phorum | Multiple PHP remote file inclusion vulnerabilities in Phorum 5.1.14, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via unspecified vectors related to an uninitialized variable. | unknown 2006-07-18 | 5.6 | CVE-2006-3615 OTHER-REF |
| Pixelated By Lev -- Pixelated By Lev Guestbook | Cross-site scripting (XSS) vulnerability in pblguestbook.php in Pixelated By Lev (PBL) Guestbook 1.32 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) name, (2) message (aka comments), (3) website, and (4) email parameters, which bypasses XSS protection mechanisms that check for SCRIPT tags but not others, as demonstrated by a javascript URI in an onMouseOver attribute and the src attribute in an iframe tag. NOTE: some vectors might overlap CVE-2006-2975, although the use of alternate manipulations makes it unclear. | unknown 2006-07-18 | 4.7 | CVE-2006-3617 BUGTRAQ OTHER-REF |
| Rocks Clusters -- Rocks Clusters | Rocks Clusters 4.1 and earlier allows local users to gain privileges via commands enclosed with escaped backticks (`) in an argument to the (1) mount-loop (mount-loop.c) or (2) umount-loop (umount-loop.c) command, which is not filtered in a system function call. | unknown 2006-07-21 | 4.9 | CVE-2006-3693 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF |

| | | | | |
|--|---|-----------------------|---------------------|---|
| Seyeon -- FlexWATCH Network Camera | Cross-site scripting (XSS) vulnerability in index.php in FlexWATCH Network Camera 3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the URL. | unknown 2006-07-18 | 4.7 | CVE-2006-3603 BUGTRAQ OTHER-REF BID SECUNIA XF |
| Yukihiro Matsumoto -- Ruby | Multiple unspecified vulnerabilities in Ruby before 1.8.5 allow remote attackers to bypass "safe level" checks via unspecified vectors involving (1) the alias function and (2) "directory operations". | unknown 2006-07-21 | 4.7 | CVE-2006-3694 OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF |

[Back to top](#)

| Low Vulnerabilities | | | | |
|--|---|-----------------------|---------------------|---|
| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
| Agnitum -- Outpost Pro Firewall | filtnt.sys in Outpost Firewall Pro before 3.51.759.6511 (462) allows local users to cause a denial of service (crash) via long arguments to mshta.exe. | unknown 2006-07-21 | 1.6 | CVE-2006-3696 BUGTRAQ BID FRSIRT SECUNIA |
| Armagetron -- Armagetron Advanced | nNetObject.cpp in Armagetron Advanced 2.8.2 and earlier allows remote attackers to cause a denial of service (application crash) via a large owner value, which causes an assert error. | unknown 2006-07-18 | 2.3 | CVE-2006-3673 ALTERVISTA FRSIRT SECUNIA |
| Armagetron -- Armagetron Advanced | nNetObject.cpp in Armagetron Advanced 2.8.2 and earlier allows remote attackers to cause a denial of service (CPU consumption) via a large number handled by the id_req_handler function. | unknown 2006-07-18 | 3.3 | CVE-2006-3674 ALTERVISTA FRSIRT SECUNIA |
| AWStats -- AWStates | Multiple cross-site scripting (XSS) vulnerabilities in awstats.pl in AWStats 6.5 build 1.857 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) refererpagesfilter, (2) refererpagesfilterex, (3) urlfilterex, (4) urlfilter, (5) hostfilter, or (6) hostfilterex parameters, a different set of vectors than CVE-2006-1945. | unknown 2006-07-21 | 1.9 | CVE-2006-3681 OTHER-REF FRSIRT SECUNIA XF |
| AWStats -- AWStats | awstats.pl in AWStats 6.5 build 1.857 and earlier allows remote attackers to obtain the installation path via the (1) year, (2) pluginmode or (3) month parameters. | unknown 2006-07-21 | 2.3 | CVE-2006-3682 OTHER-REF FRSIRT SECUNIA XF |
| Carbonize Lazarus -- Carbonize Lazarus | Multiple cross-site scripting (XSS) vulnerabilities in Carbonize Lazarus Guestbook 1.6 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the show parameter in codes-english.php and (2) | unknown 2006-07-18 | 2.3 | CVE-2006-3616 BUGTRAQ BID |

| | | | | |
|--|---|--------------------------|---------------------|--|
| Guestbook | the img parameter in picture.php, after the name of an existing file. | | | |
| Cisco -- Unified CallManager | The command line interface (CLI) in Cisco Unified CallManager (CUCM) 5.0(1) through 5.0(3a) allows local users to overwrite arbitrary files by redirecting a command's output to a file or folder, aka bug CSCse31704. | unknown 2006-07-18 | 1.4 | CVE-2006-3593 CISCO FRSIRT SECUNIA XF |
| Cisco -- Intrusion Prevention System | The device driver for Intel-based gigabit network adapters in Cisco Intrusion Prevention System (IPS) 5.1(1) through 5.1(p1), as installed on various Cisco Intrusion Prevention System 42xx appliances, allows remote attackers to cause a denial of service (kernel panic and possibly network outage) via a crafted IP packet. | unknown 2006-07-18 | 2.3 | CVE-2006-3596 CISCO BID FRSIRT SECUNIA XF |
| CutePHP -- CuteNews | Cross-site scripting (XSS) vulnerability in Index.PHP in CuteNews 1.4.5 allows remote attackers to inject arbitrary web script or HTML via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown 2006-07-18 | 1.9 | CVE-2006-3661 OTHER-REF BID |
| Deerfield -- VisNetic Mail Server MERAK -- Mail Server IceWarp -- Web Mail | Absolute path directory traversal vulnerability in (a) MERAK Mail Server for Windows 8.3.8r with before IceWarp Web Mail 5.6.1 and (b) VisNetic MailServer before 8.5.0.5 allows remote attackers to include arbitrary files via a full Windows path and drive letter in the (1) language parameter in accounts/inc/include.php and (2) lang_settings parameter in admin/inc/include.php, which is not properly sanitized by the securepath function, a related issue to CVE-2005-4556. | 2006-02-21 2006-07-21 | 2.3 | CVE-2006-0817 OTHER-REF OTHER-REF BID FRSIRT SECUNIA SECUNIA |
| Deerfield -- VisNetic Mail Server MERAK -- Mail Server IceWarp -- Web Mail | Absolute path directory traversal vulnerability in (1) MERAK Mail Server for Windows 8.3.8r with before IceWarp Web Mail 5.6.1 and (2) VisNetic MailServer before 8.5.0.5 allows remote authenticated users to include arbitrary files via a modified language parameter and a full Windows or UNC pathname in the lang_settings parameter to mail/index.html, which is not properly sanitized by the validatefolder PHP function, possibly due to an incomplete fix for CVE-2005-4558. | 2006-02-21 2006-07-21 | 1.4 | CVE-2006-0818 OTHER-REF OTHER-REF BID FRSIRT SECUNIA SECUNIA |
| dream4 -- Koobi Pro | Cross-site scripting (XSS) vulnerability in the showtopic module in Koobi Pro CMS 5.6 allows remote attackers to inject arbitrary web script or HTML via the toid parameter. | unknown 2006-07-18 | 1.9 | CVE-2006-3620 BID SECTRACK |
| Ethereal Group -- Ethereal | Unspecified vulnerability in the GSM BSSMAP dissector in Wireshark (formerly Ethereal) 0.10.11 to 0.99.0 allows remote attackers to cause a denial of service (crash) via unspecified vectors. | unknown 2006-07-21 | 3.3 | CVE-2006-3627 WIRESHARK |
| Ethereal Group -- Ethereal | Unspecified vulnerability in the MOUNT dissector in Wireshark (formerly Ethereal) 0.9.4 to 0.99.0 allows remote attackers to cause a denial of service (memory | unknown 2006-07-21 | 2.3 | CVE-2006-3629 WIRESHARK |

| | | | | |
|---|---|--------------------------|---------------------|---|
| | consumption) via unspecified vectors. | | | |
| Ethereal Group -- Ethereal | Unspecified vulnerability in the SSH dissector in Wireshark (formerly Ethereal) 0.9.10 to 0.99.0 allows remote attackers to cause a denial of service (infinite loop) via unknown attack vectors. | unknown 2006-07-21 | 3.3 | CVE-2006-3631 WIRESHARK |
| FarsiNews -- FarsiNews | Directory traversal vulnerability in jscripits/tiny_mce/tiny_mce_gzip.php in FarsiNews 3.0 BETA 1 allows remote attackers to include arbitrary files via a .. (dot dot) sequence and trailing null (%00) byte in the language parameter in the advanced theme. | unknown 2006-07-18 | 2.3 | CVE-2006-3602 BUGTRAQ BID SECTrack XF |
| FlatNuke -- FlatNuke | The Gallery module in Simone Vellei Flatnuke 2.5.7 and earlier, when Gallery uploads are enabled, does not restrict the extensions of uploaded files that begin with a GIF header, which allows remote authenticated users to execute arbitrary PHP code via an uploaded .php file. | 2006-07-12 2006-07-18 | 3.4 | CVE-2006-3608 BUGTRAQ ALTERVISTA BID |
| FLV -- FLV Player | Multiple cross-site scripting (XSS) vulnerabilities in FLV Players 8 allow remote attackers to inject arbitrary web script or HTML via the url parameter to (1) player.php or (2) popup.php. | unknown 2006-07-18 | 2.3 | CVE-2006-3624 BUGTRAQ BID |
| FLV -- FLV Player | FLV Players 8 allows remote attackers to obtain sensitive information via (1) a direct request to paginate.php or (2) an invalid p parameter to player.php, which reveal the path in an error message. | unknown 2006-07-18 | 2.3 | CVE-2006-3625 BUGTRAQ |
| HP -- OpenVMS | Unspecified vulnerability in [SYSEXEC]SMPUTIL.EXE in HP OpenVMS 7.3-2 allows local users and "remote users" to cause a denial of service (crash). | unknown 2006-07-21 | 2.3 | CVE-2006-3686 OTHER-REF FRSIRT SECUNIA |
| KDE -- Konqueror | KDE Konqueror 3.5.1 and earlier allows remote attackers to cause a denial of service (application crash) by calling the replaceChild method on a DOM object, which triggers a null dereference, as demonstrated by calling document.replaceChild with a 0 (zero) argument. | unknown 2006-07-18 | 1.9 | CVE-2006-3672 BLOGSPOT BID FRSIRT OSVDB XF |
| Koobi -- Koobi Pro | The showtopic module in Koobi Pro CMS 5.6 allows remote attackers to obtain sensitive information via a ' (single quote) in the p parameter, which displays the path in an error message. NOTE: it is not clear whether this is SQL injection or a forced SQL error. | unknown 2006-07-18 | 2.3 | CVE-2006-3622 SECTrack |
| Linux -- Linux kernel | Linux kernel 2.6.x, when using both NFS and EXT3, allows remote attackers to cause a denial of service (file system panic) via a crafted UDP packet with a V2 lookup procedure that specifies a bad file handle (inode number), which triggers an error and causes an exported directory to be remounted read-only. | unknown 2006-07-21 | 3.3 | CVE-2006-3468 OTHER-REF OTHER-REF |
| McAfee -- ePolicy Orchestrator Agent | Directory traversal vulnerability in Framework Service component in McAfee ePolicy Orchestrator agent 3.5.0.x and earlier allows remote attackers to create arbitrary files via a .. (dot dot) in the directory and filename in a | unknown 2006-07-18 | 2.3 | CVE-2006-3623 OTHER-REF FRSIRT SECUNIA |

| | | | | |
|--|---|--------------------------|---------------------|--|
| | PropsResponse (PackageType) request. | | | |
| Mercury Messenger -- Mercury Messenger | Mercury Messenger, possibly 1.7.1.1 and other versions, when running on a multi-user Mac OS X platform, stores chat logs with world-readable permissions within the /Users directory, which allows local users to read the chat logs from other users. | unknown 2006-07-18 | 1.6 | CVE-2006-3669 BUGTRAQ |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (application crash) by accessing the URL property of a TriEditDocument.TriEditDocument object before it has been initialized, which triggers a NULL pointer dereference. | unknown 2006-07-18 | 2.3 | CVE-2006-3591 OTHER-REF BID FRSIRT OSVDB |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (crash) by setting the Transition property on an uninitialized DXImageTransform.Microsoft.RevealTrans.1 ActiveX Object, which triggers a null dereference. | unknown 2006-07-18 | 2.3 | CVE-2006-3605 OTHER-REF BID FRSIRT OSVDB XF |
| Microsoft -- Works Spreadsheet | wksss.exe 8.4.702.0 in Microsoft Works Spreadsheet 8.0 allows remote attackers to cause a denial of service (CPU consumption or crash) via crafted (1) Works, (2) Excel, and (3) Lotus 1-2-3 files. | 2006-07-10 2006-07-18 | 1.9 | CVE-2006-3653 BUGTRAQ BID FRSIRT |
| Microsoft -- Works Spreadsheet | Buffer overflow in wksss.exe 8.4.702.0 in Microsoft Works Spreadsheet 8.0 allows remote attackers to cause a denial of service (CPU consumption or crash) via crafted Excel files. | 2006-07-10 2006-07-18 | 1.9 | CVE-2006-3654 BUGTRAQ BID FRSIRT |
| Microsoft -- PowerPoint | Unspecified vulnerability in Microsoft PowerPoint 2003 allows user-complicit attackers to cause memory corruption via a crafted PowerPoint file, which triggers the corruption when the file is closed. NOTE: due to the lack of available details as of 20060717, it is unclear how this is related to CVE-2006-3655, CVE-2006-3660, and CVE-2006-3590, although it is possible that they are all different. | unknown 2006-07-18 | 1.9 | CVE-2006-3656 BUGTRAQ BID FRSIRT |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (stack overflow exception) via a DXImageTransform.Microsoft.Gradient ActiveX object with a long (1) StartColorStr or (2) EndColorStr property. | unknown 2006-07-18 | 2.3 | CVE-2006-3657 FRSIRT OSVDB |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (crash) by accessing the object references of a FolderItem ActiveX object, which triggers a null dereference in the security check. | unknown 2006-07-18 | 2.3 | CVE-2006-3658 OTHER-REF FRSIRT OSVDB |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (crash) by setting the location or URL property of a MHTMLFile ActiveX object. | unknown 2006-07-18 | 2.3 | CVE-2006-3659 OTHER-REF FRSIRT OSVDB |

| | | | | |
|----------------------------------|---|-----------------------|---------------------|--|
| MySQL -- MySQL | Format string vulnerability in time.cc in MySQL Server 4.1 before 4.1.21 and 5.0 before 1 April 2006 allows remote authenticated users to cause a denial of service (crash) via a format string instead of a date as the first parameter to the date_format function, which is later used in a formatted print call to display the error message. | unknown 2006-07-21 | 1.4 | CVE-2006-3469 OTHER-REF DEBIAN OTHER-REF OTHER-REF |
| Orbitcoders -- OrbitMATRIX | Cross-site scripting (XSS) vulnerability in index.php in Orbitcoders OrbitMATRIX 1.0 allows remote attackers to inject arbitrary web script or HTML via the page_name parameter with an IMG tag containing a javascript URI in the SRC attribute. | unknown 2006-07-18 | 2.3 | CVE-2006-3609 BUGTRAQ XF |
| Orbitcoders -- OrbitMATRIX | index.php in Orbitcoders OrbitMATRIX 1.0 allows remote attackers to obtain sensitive information (partial database schema) via a modified page_name parameter, which reflects portions of an SQL query in the result. NOTE: it is not clear whether the information is target-specific. If not, then this issue is not an exposure. | unknown 2006-07-18 | 2.3 | CVE-2006-3610 BUGTRAQ |
| Phorum -- Phorum | Directory traversal vulnerability in pm.php in Phorum 5 allows remote authenticated users to include and execute arbitrary local files via directory traversal sequences in the GLOBALS[template] parameter, as demonstrated by injecting PHP sequences into a log file, which is then included by pm.php. | unknown 2006-07-18 | 2.8 | CVE-2006-3611 BUGTRAQ ALTERVISTA PHORUM FRSIRT |
| Phorum -- Phorum | Cross-site scripting (XSS) vulnerability in Phorum 5.1.14 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown 2006-07-18 | 1.9 | CVE-2006-3612 PHORUM |
| Photocycle -- Photocycle | Cross-site scripting (XSS) vulnerability in photocycle in Photocycle 1.0 allows remote attackers to inject arbitrary web script or HTML via the phpage parameter. | unknown 2006-07-21 | 1.9 | CVE-2006-3680 BUGTRAQ |
| SoftBiz -- Banner Exchange | Multiple cross-site scripting (XSS) vulnerabilities in Softbiz Banner Exchange Script (aka Banner Exchange Network Script) 1.0 allow remote attackers to inject arbitrary web script or HTML via (1) the city parameter in (a) insertmember.php, and (2) a PHPSESSID cookie in (b) lostpassword.php, (c) gen_confirm_mem.php, and (d) index.php. | unknown 2006-07-18 | 2.3 | CVE-2006-3607 BUGTRAQ OTHER-REF BID XF XF |
| SquirrelMail -- SquirrelMail | SquirrelMail 1.4.6 and earlier, with register_globals enabled, allows remote attackers to hijack cookies in src/redirect.php via unknown vectors. NOTE: while "cookie theft" is frequently associated with XSS, the vendor disclosure is too vague to be certain of this. | unknown 2006-07-18 | 1.9 | CVE-2006-3665 OTHER-REF FRSIRT |
| Sun -- Solaris | Unspecified vulnerability in Sun Solaris X Inter Client Exchange library (libICE) on Solaris 8 and 9 allows context-dependent attackers to cause a denial of service (application crash) to applications that use the library. | unknown 2006-07-18 | 2.3 | CVE-2006-3606 SUNALERT |
| Sun -- Solaris | Unspecified vulnerability in NIS server on Sun Solaris 8, 9, and 10 allows local and remote attackers to cause a denial of service (ypserv hang) via unknown vectors. | unknown 2006-07-18 | 2.3 | CVE-2006-3664 SUNALERT BID |

| | | | | |
|--|---|--------------------------|---------------------|--|
| | | | | FRSIRT SECTRACK SECUNIA XF |
| Sun -- Solaris | Unspecified vulnerability in the kernel in Solaris 10 with patch 118822-29 (118844-29 on x86) before patch 118833-11 (118855-08) allows remote authenticated users to cause a denial of service via unspecified vectors that lead to "kernel data structure corruption" that can trigger a system panic, application failure, or "data corruption." | unknown 2006-07-21 | 2.0 | CVE-2006-3728 SUNALERT BID FRSIRT SECUNIA |
| Symantec -- Norton Personal Firewall | Norton Personal Firewall 2006 9.1.0.33 allows local users to cause a denial of service (crash) via certain RegSaveKey, RegRestoreKey and RegDeleteKey operations on the (1) HKLM\SYSTEM\CurrentControlSet\Services\SNDSrvc and (2) HKLM\SYSTEM\CurrentControlSet\Services\SymEvent registry keys. | 2006-07-15 2006-07-21 | 1.6 | CVE-2006-3725 BUGTRAQ OTHER-REF |
| VMWare -- ESX Server VMWare -- VMWare Infrastructure VMWare -- VMWare Workstation VMWare -- VMWare Server VMWare -- Player | vmware-config.pl in VMware for Linux, ESX Server 2.x, and Infrastructure 3 does not check the return code from a Perl chmod function call, which might cause an SSL key file to be created with an unsafe umask that allows local users to read or modify the SSL key. | unknown 2006-07-21 | 3.3 | CVE-2006-3589 BUGTRAQ OTHER-REF BID BID SECUNIA |

[Back to top](#)

Last updated July 24, 2006